REMARKS

In response to the Office Action mailed November 29, 2007, Applicant respectfully requests reconsideration. Claims 1-33 and 37-39 were previously pending in this application. By this amendment, claims 1, 19, 21, 24, and 37 have been amended. Claim 38 has been canceled. As a result, claims 1-33, 37 and 39 are pending for examination with claims 1, 19, 21, and 37 being independent. No new matter has been added.

Rejections under 35 U.S.C. §112

The Office Action rejected claim 24 as having a limitation with insufficient antecedent basis. Applicant has amended claim 24 to address the rejection.

Accordingly, withdrawal of this rejection is respectfully requested.

I. Rejections Under 35 U.S.C. §103

The Office Action rejects claims 1-5, 7-15, and 18-20 under 35 U.S.C. 103(a) as allegedly being unpatentable over Coley et al., U.S. Patent No. 5,826,014, (hereinafter "Coley"), and further in view of Montenegro, U.S. Patent No. 6,233,688, (hereinafter "Montenegro"). Applicant respectfully disagrees. In addition, Applicant has amended independent claims 1 and 19 to more clearly distinguish over the cited references.

A. Independent Claim 1

Claim 1, as amended, recites:

> A computer-implemented method, comprising:
>
> *receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system*, a call from an application *via a first application programming interface*, the call having parameters for a connection to an endpoint that the application desires to establish, *whereby the application explicitly communicates a request to traverse a firewall to establish the connection*; and
>
> making, by the operating system and/or the enforcement module, a call *via a second application programming* interface to the firewall to establish the connection in accordance with the parameters.
>
> (Emphasis added).

On page 5, the Office Action alleges that Coley teaches limitations of claim 1. Specifically, the Office Action points out that Coley teaches, in col. 7, lines 5-20 and 37, and in col. 8, lines 3-4 and 6-12 receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application via a first application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to establish the connection.

Coley discusses a firewall that is a **stand-alone system** that physically resides between a point of public access and a network element to be protected. (Coley, col. 5, lines 51-54). (Emphasis added). A user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall 210. (Coley, Fig. 2; col. 7, lines 16-18). A dedicated firewall computing platform is referred to as a "firewall box." (Coley, col. 5, lines 56-58). The firewall application running on the firewall box is comprised of a plurality of proxy agents. (Coley, col. 6, lines 4-5). In a preferred embodiment, individual proxy agents are assigned to designated ports to monitor, respond to and verify incoming access requests (i.e., incoming packets) received on the port. (Coley, col. 6, lines 5-8). Proxy agents investigate incoming requests that seek to access network elements residing behind the firewall 210. (Coley, Fig. 2; col. 7, lines 37-39). The proxy agent assigned to a port performs all of the verification processes and management of the port **without involving the operating system**, or a port manager (as in conventional systems). (Coley, col. 7, lines 47-50). (Emphasis added). In contrast, claim 1 recites receiving, by *an operating system* and/or an enforcement module which is associated with or is *part of the operating system*, a call from an application. (Emphasis added).

Further, claim 1 has been amended to recite whereby the application explicitly communicates *a request to traverse a firewall* to establish the connection. (Emphasis added). Coley does not teach or suggest this limitation. Therefore, Coley does not teach or suggest “a computer-implemented method, comprising: receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application via a first application programming interface, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to traverse a firewall to establish the connection; and making, by the operating system and/or the enforcement module, a call via a second application programming interface to the firewall to establish the connection in accordance with the parameters," as recited in claim 1.

The Office Action concedes that Coley does not explicitly teach an application programming interface. The Office Action then states that Montenegro "teaches a firewall traversal method regarding loading an application programming interface (API) onto the client system" in col. 7, lines 17-20. In this portion, Montenegro discusses that if the specific "raft-type" (type of firewall traversal and/or remote access security, see above) is not provided for in the socket factory, by way of methods, functions, classes and/or code that can be executed, then the required methods, functions, classes, code, etc. must be obtained. (Montenegro, col. 7, lines 11-15). In that case, the firewall traversal procedure first gets the needed methods, classes, etc. for the raft-type. (Montenegro, col. 7, lines 15-17). These methods, classes, etc. may be obtained from the firewall itself and then loaded as an API (Application Program Interface) or mobile code, such as Java applet, onto the client system. (Montenegro, col. 7, lines 17-20). However, Montenegro does not teach or suggest that this API is either used for receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from an application or making, by the operating system and/or the enforcement module, a call … to the firewall, as recited in claim 1.

Montenegro also discusses that the client application 310 makes use of a socket factory 320 (Application Program Interface) to access a system resource such as sockets. (Montenegro, col. 4, lines 50-52). The socket factory recognizes the RAFT URL (see FIG. 5) and configures itself 330 to communicate with gateway/firewall 350. (Montenegro, col. 4, lines 60-62). Thus, the socket factory Montenegro is itself an API and Montenegro does not teach receiving, *by an operating system and/or an enforcement module which is associated with or is part of the operating system*, a call from an application *via a first application programming interface*, as recited in claim 1.

In view of the foregoing, claim 1 patentably distinguishes over Coley and Montenegro, either alone or in combination.

Claims 2-18 depend from claim 1 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 1-18 is respectfully requested.

B. <u>Independent Claim 19</u>

Claim 19, as amended, recites:

> A computer system comprising:
> an operating system;
> *a first application programming interface associated with the operating system and configured and adapted to receive a call from an application*, the call having parameters for a connection to an endpoint that the application desires to establish, *whereby the application explicitly communicates a request to traverse a firewall to establish the connection*; and
> an enforcement module associated with or is part of the operating system and called via the application programming interface and configured and adapted to:
> receive an indication from the application that the application desires to establish the connection; and
> *make a call via a second application programming interface to a firewall* to establish the connection in accordance with the parameters.
> (Emphasis added).

On page 8, the Office Action states that claim 19 is rejected "because it is directed to the same subject matter as claim 1." Claim 19 has been amended to recite that the application explicitly communicates a request to traverse a firewall to establish the connection.

As should be clear from the above discussion in connection with claim 1, neither Coley nor Montenegro teach or suggest "a first application programming interface associated with the operating system and configured and adapted to receive a call from an application, the call having parameters for a connection to an endpoint that the application desires to establish, whereby the application explicitly communicates a request to traverse a firewall to establish the connection; and an enforcement module associated with or is part of the operating system and called via the application programming interface and configured and adapted to: receive an indication from the application that the application desires to establish the connection; and make a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters," as recited in claim 19.

In view of the foregoing, claim 19 patentably distinguishes over Coley and Montenegro, either alone or in combination.

Claim 20 depends from claim 19 and is allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 19 and 20 is respectfully requested.

II. Rejections Under 35 U.S.C. §103

The Office Action rejected claims 21-26, 30, 33, and 37-38 under 35 U.S.C. 103(a) as being unpatentable over Malcolm, U.S. Patent No. 7,146,638, (hereinafter "Malcolm"), and further in view of Montenegro. Applicant respectfully disagrees. In addition, Applicant has amended claims 21 and 37 to more clearly distinguish over the cited references.

A. Independent Claim 21

Claim 21, as amended, recites:

> A computer-implemented method, comprising:
>
> receiving, *by an interception module communicating with a firewall via a first application programming interface* and including *a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module*, and a filter cache, a connect attempt, a listen attempt, or a combination thereof from an application or a service;
>
> extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof;
>
> identifying, *by the interception module*, the user and the application or the service from the user and application or service information;
>
> evaluating, *by the interception module,* the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies; and
>
> if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, *instructing, by the interception module, the firewall to create a configuration* to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache.
>
> (Emphasis added).

On page 9, the Office Action states that Malcolm teaches limitations of claim 21. However, Malcolm discusses that the **firewall receives the at least one access request definition from the application program** during startup of the application program or immediately prior to the intercepted access request (Malcolm, col. 4, lines 20-25). (Emphasis added). Specifically, **the application program will preferably provide the firewall program** with a list of Internet access requests that the application may possibly have during execution of the application (Malcolm, col. 6, lines 41-44). (Emphasis added). In contrast, claim 21, as amended, recites receiving, *by an interception module communicating with a firewall via a first application programming interface* and including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache, and a filter cache, *a connect attempt, a listen attempt, or a combination thereof from an application or a service.* (Emphasis added). Therefore, while Malcolm describes that the firewall receives the at least one access request definition from the application program (Malcolm, col. 4, lines 20-22), claim 21 recites receiving, by an interception module communicating with a firewall via a first application programming interface ... a connect attempt, a listen attempt, or a combination thereof from an application or a service.

Furthermore, on page 10, the Office Action notes that "approving/denying of access requests based from evaluating access requests against access rules that covers such requests is evidence that configurations have been created for those requests. Examiner also notes that access rules read on firewall policies." Claim 21 recites "... an interception module ... including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module" and "evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies." Moreover, claim 21 recites "an interception module ... including ... a filter cache" and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, *instructing, by the interception module, the firewall to create a configuration* to allow the connect attempt, the listen attempt, or the combination thereof, and *storing the configuration in the filter cache.* (Emphasis added). Malcolm, however, describes that **the firewall program accesses its access rules** data structure and determines whether there is already an access rule covering the type of access request received from the application (Malcolm, col. 9, lines 38-41). (Emphasis added). Therefore, Malcolm does not teach or suggest "receiving, by an interception module communicating with a firewall via a first application programming interface and including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module, and a filter cache, a connect attempt, a listen attempt, or a combination thereof from an application or a service; ... identifying, by the interception module, the user and the application or the service from the user and application or service information; evaluating, by the interception module, the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing, by the interception module, the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache," as recited in claim 21.

The Office Action concedes that Malcolm does not explicitly teach an application programming interface. The Office Action then states that Montenegro "teaches a firewall traversal method regarding loading an application programming interface (API) onto the client system" in col. 7, lines 17-20. However, Montenegro does not teach "an interception module communicating with a firewall via a first application programming interface and including a second application programming interface," as recited in claim 21.

In view of the foregoing, claim 21 patentably distinguishes over Malcolm and Montenegro, either alone or in combination.

Claims 22-33 depend from claim 21 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 21-33 is respectfully requested.

D. Independent Claim 37

Claim 37, as amended, recites:

> A computer system, comprising:
> a firewall; and
> *an interception module communicating with the firewall via a first application programming interface*, the interception module including *a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module*, and a filter cache and configured and adapted to:
>
> intercept a request for a connect attempt, a listen attempt, or a combination thereof from the application or the service;

> extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof;
>
> identify the user and the application or the service from the user and application or service information;
>
> evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and
>
> if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache.
>
> (Emphasis added).

On page 12, the Office Action rejects claim 37 as directed to the same subject matter as claims 21. As should be clear form the above discussion in connection with claim 21, neither Malcolm nor Montenegro teach or suggest "an interception module communicating with the firewall via a first application programming interface, the interception module including a second application programming interface for at least one of a user, an application and a service to establish at least one policy from a plurality of policies stored in a policy cache of the interception module, and a filter cache and configured and adapted to: intercept a request for a connect attempt, a listen attempt, or a combination thereof from the application or the service; extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof; identify the user and the application or the service from the user and application or service information; evaluate the application or service information to determine if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from a plurality of policies; and if the connect attempt, the listen attempt, or the combination thereof comply with one or more policies from the plurality of policies, instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in the filter cache," as recited in claim 37.

In view of the foregoing, claim 37 patentably distinguishes over Malcolm and Montenegro, either alone or in combination.

Claim 39 depends from claim 37 and is allowable for at least the same reasons.

Accordingly, withdrawal of the rejection of claims 37 and 39 is respectfully requested.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: February 29, 2008

Respectfully submitted,

By:
James H. Morris, Reg. No. 34,681
Wolf, Greenfield & Sacks, P.C.
Federal Reserve Plaza
00 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000